Purity and Proof Theory (I): Three euclidian proofs of IP

Mirko Engler

Remark: Certainly, to discuss purity and simplicity of proofs in a formal manner, one needs a criteria of identity of proofs, that goes beyond syntactical equality and is stricter than proving the same theorem. We won't give such a criteria here. Nevertheless, that doesn't mean, we can not investigate some general properties of proofs. In fact, we will speak of provability in axiomatic theories, which so to speak provide certain proofs, that are clearly to be distinguished by their applied reasoning - no matter how to define identity of proofs precisely.

1 Formal Arithmetic

1.1 Definitions

The language of arithmetic is defined as $L[\mathrm{PA}] := L[0, S, +, \times]$. The theory $\overline{\mathrm{PA}}^{L[\mathrm{PA}]}$ is the deductive closer of the following axioms under 1.-order classical logic in the language of $L[\mathrm{PA}]$:

(PA 1) $\forall x(Sx \neq 0)$
(PA 2) $\forall x(x + 0 = x)$
(PA 3) $\forall x(x \times 0 = 0)$
(PA 4) $\forall xy(Sx = Sy \to x = y)$
(PA 5) $\forall xy(x + Sy = S(x + y))$
(PA 6) $\forall xy(x \times Sy = x \times y + x)$
(Ind) $\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(Sx)) \to \forall x\varphi$ for φ in $L[\mathrm{PA}]$

Definition 1.1. We extend $L[\mathrm{PA}]$ by the following definitions to $L[\mathrm{PA}]^+$:

- $1 := S(0)$
- $x \leq y :\leftrightarrow \exists z_{\leq y}(z + x = y)$
- $x > y :\leftrightarrow \neg x \leq y$
- $x|y :\leftrightarrow x > 0 \wedge \exists! z_{\leq y}(z \times x = y)$
- $P(x) :\leftrightarrow x > 1 \wedge \forall y_{\leq x}(y|x \to y = x \vee y = 1)$
- $\prod_{i=1}^{x} p_i := p_1 \times ... \times p_n$ for the first n primes, such that $p_n \leq SSx$
- $x - y := \begin{cases} \iota z(z + y = x), \text{ if } x > y \\ \text{undefinded, otherwise} \end{cases}$

Furthermore we can formulate in the language of $L[\mathrm{PA}]^+$ the schema

$$(<-Ind)\ \ \forall x[\forall y(y<x\to\varphi(y))\to\varphi(x)]\to\forall x\varphi$$

for φ in $L[\mathrm{PA}]$, which is equivalent to (Ind) over $\overline{\mathrm{PA}}^{L[\mathrm{PA}]^+}$. Recognize that $\overline{\mathrm{PA}}^{L[\mathrm{PA}]^+}$ is just an extension of $\overline{\mathrm{PA}}^{L[\mathrm{PA}]}$ by definitions. We won't differentiate between them and only speak of PA. Furthermore it will be interesting to distinguish between variants of PA wich use weaker induction, i.e. induction restricted to formulas of a certain arithmetical complexity. These theories will be denoted by $\mathrm{I}\Sigma_n^0$ if they allow for induction up to Σ_n^0-formulas.

1.2 Basic Lemmata

First, we prove some basic principles, which are helpfull to give Euclids version of the proof of IP in PA.

Lemma 1.2. $\mathrm{PA}\vdash\forall x(x\neq Sx)$

Proof. By (PA 1) it is the case that

$$\mathrm{PA}\vdash\forall x(Sx\neq 0) \tag{1}$$
$$\mathrm{PA}\vdash S0\neq 0 \tag{2}$$

By contraposition of (PA 4) it follows that

$$\mathrm{PA}\vdash\forall xy(x\neq y\to Sx\neq Sy) \tag{3}$$
$$\mathrm{PA}\vdash\forall x(x\neq Sx\to Sx\neq SSx) \tag{4}$$

and using the Induction-Schema we finally conclude that

$$\mathrm{PA}\vdash S0\neq 0\wedge\forall x(x\neq Sx\to Sx\neq SSx)\to\forall x(x\neq Sx) \tag{5}$$
$$\mathrm{PA}\vdash\forall x(x\neq Sx) \tag{6}$$

□

Lemma 1.3. $\mathrm{PA}\vdash\forall xy(x<S(y)\leftrightarrow x\leq y)$

.
.

Lemma 1.4. $\mathrm{PA}\vdash\forall x(x>1\to\exists y(Py\wedge y|x))$

Proof. Because $\mathrm{PA}\vdash x|x$ we conclude that

$$\mathrm{PA}\vdash Px\to\exists z(Pz\wedge z|x) \tag{7}$$

By definition of Px it follows that

$$\mathrm{PA}\vdash\neg Px\to(x>1\to\exists v(v<x\wedge v|x)) \tag{8}$$
$$\mathrm{PA}\vdash\forall y(y<x\to\exists z(Pz\wedge z|y))\to(\exists v(v<x\wedge v|x\to\exists z(Pz\wedge z|v)) \tag{9}$$

since PA $\vdash \forall xvz(v|x \to (z|v \to z|x))$, we conclude that

$$\text{PA} \vdash \neg Px \to [x > 1 \to (\forall y(y < x \to \exists z(Pz \wedge z|y)) \to \exists z(Pz \wedge z|x))] \tag{10}$$

And since PA $\vdash Px \vee \neg Px$ by logic

$$\text{PA} \vdash \forall x[x > 1 \to \forall y(y < x \to \exists z(Pz \wedge z|y)) \to \exists z(Pz \wedge z|x)] \tag{11}$$

Using ($<$ - Ind) with $x > 1$, we conclude that

$$\begin{aligned} &\text{PA} \vdash \forall x[x > 1 \to (\forall y(y < x \to \exists z(Pz \wedge z|y)) \to \exists z(Pz \wedge z|x)] \\ &\qquad \to \forall x(x > 1 \to \exists y(Py \wedge y|x))) \end{aligned} \tag{12}$$

$$\text{PA} \vdash \forall x(x > 1 \to \exists y(Py \wedge y|x)) \tag{13}$$

□

Lemma 1.5. PA $\vdash \forall xy(y|x \wedge y|Sx \to y = 1)$

Proof.

$$\text{PA} \vdash u \times y = x \wedge v \times y = S(x) \to (x < S(x) \to u < v) \tag{14}$$

$$\text{PA} \vdash x < S(x) \tag{15}$$

$$\text{PA} \vdash u \times y = x \wedge v \times y = S(x) \to u < v \tag{16}$$

By PA 6 we conclude that

$$\text{PA} \vdash y > 1 \to S(y \times u) < y \times S(u) \tag{17}$$

$$\text{PA} \vdash u < v \to S(u) \leq v \tag{18}$$

$$\text{PA} \vdash S(u) \leq v \to y \times S(u) \leq y \times v \tag{19}$$

By PA-provable transitivity of $<$ we conclude that

$$\text{PA} \vdash S(y \times u) < y \times S(u) \to (y \times S(u) \leq y \times v \to S(y \times u) < y \times v) \tag{20}$$

$$\text{PA} \vdash u < v \to (y > 1 \to S(y \times u) < y \times v) \tag{21}$$

$$\text{PA} \vdash S(y \times u) < y \times v \to S(x) < S(x) \tag{22}$$

$$\text{PA} \vdash S(x) < S(x) \to \bot \tag{23}$$

$$\text{PA} \vdash u < v \to y \leq 1 \tag{24}$$

$$\text{PA} \vdash u \times y = x) \wedge \forall v(v \times y = S(x) \to y \leq 1 \tag{25}$$

$$\begin{aligned} &\text{PA} \vdash (\forall uv(u \times y = x \wedge v \times y = S(x)) \to y \leq 1) \to \\ &\qquad (\exists uv(u \times y = x \wedge v \times y = S(x)) \to y \leq 1) \end{aligned} \tag{26}$$

$$\text{PA} \vdash y|x \wedge y|S(x) \to y > 0 \wedge \exists uv(u \times y = x \wedge v \times y = S(x)) \tag{27}$$

$$\text{PA} \vdash y|x \wedge y|S(x) \to y > 0 \wedge y \leq 1 \tag{28}$$

$$\text{PA} \vdash \forall yx(y|x \wedge y|S(x) \to y = 1) \tag{29}$$

□

2 Euclidian Proofs

2.1 Euclid's proof

Now we can give an axiomatic proof which is using only the reasoning applied by Euclid in Book IX, Proposition 20 of his Elements (see [Heath, 1908]).

Theorem 2.1. $\mathrm{PA} \vdash \forall x \exists y(y > x \wedge Py)$

Proof. By pure logic inside PA, we conclude that

$$\begin{aligned}\mathrm{PA} \vdash & \forall y(Py \to (y \leq x \to y|\prod_{i=1}^{x} p_i)) \to (\exists y(Py \wedge y|S(\prod_{i=1}^{x} p_i)) \to \\ & (\forall y(Py \to y \leq x) \to \exists y(Py \wedge y|\prod_{i=1}^{x} p_i \wedge y|S(\prod_{i=1}^{x} p_i))))\end{aligned} \tag{1}$$

With the definitions of $y|x$ and $\prod_{i=1}^{x} p_i$ it is the case that

$$\mathrm{PA} \vdash \forall y(Py \to (y \leq x \to y|(\prod_{i=1}^{x} p_i))) \tag{2}$$

By lemma 1.4 we know that $\mathrm{PA} \vdash \forall x(x > 1 \to \exists y(Py \wedge y|x))$ and by Def. of Px that $\mathrm{PA} \vdash S(\prod_{i=1}^{x} p_i) > 1$, so

$$\mathrm{PA} \vdash \exists y(Py \wedge y|S(\prod_{i=1}^{x} p_i)) \tag{3}$$

From 1, 2 and 3 it follows that

$$\mathrm{PA} \vdash \forall y(Py \to y \leq x) \to \exists y(Py \wedge y|\prod_{i=1}^{x} p_i \wedge y|S(\prod_{i=1}^{x} p_i)) \tag{4}$$

By lemma 1.5 we know that $\mathrm{PA} \vdash \forall xy(y|x \wedge y|Sx \to y = 1)$ and by Def. of Px that $\mathrm{PA} \vdash \forall y(Py \to y \neq 1)$, so

$$\mathrm{PA} \vdash \exists y(Py \wedge y|\prod_{i=1}^{x} p_i \wedge y|S(\prod_{i=1}^{x} p_i) \to \bot \tag{5}$$

$$\mathrm{PA} \vdash \forall y(Py \to y \leq x) \to \bot \tag{6}$$

$$\mathrm{PA} \vdash \forall x \exists y(Py \wedge y > x) \tag{7}$$

□

2.2 A simplified version of Euclid's proof

The proof can be cast a little differently. By definition, $\prod_{i=1}^{x} p_i$ is divisible by any prime number $p_i \leq SSx$. Suppose $S(\prod_{i=1}^{x} p_i)$, being larger than any prime number $p_i \leq SSx$, is divisible by at least one of them. Let $p_k < p_i$ be a prime-divisor of $S(\prod_{i=1}^{x} p_i)$. Then p_k divides $S(\prod_{i=1}^{x} p_i) - \prod_{i=1}^{x} p_i = 1$, a contradiction.
Formally, this amounts to giving a different proof of Lemma 1.5, which *prima facie* looks also simpler.

Proof.

$$\text{PA} \vdash y|x \wedge y|Sx \rightarrow (\iota z(z \times y = Sx) - \iota z(z \times y = x) = Sx - x) \tag{1}$$

$$\text{PA} \vdash \iota z(z \times y = Sx) - \iota z(z \times y = x) = Sx - x \rightarrow y \times (\iota z(z \times 1 = Sx) - \iota z(z \times 1 = x)) = 1 \tag{2}$$

$$\text{PA} \vdash y \times (\iota z(z \times 1 = Sx) - \iota z(z \times 1 = x)) = 1 \rightarrow \exists! z(z \times y = 1) \tag{3}$$

$$\text{PA} \vdash \forall xy(y|x \wedge y|Sx \rightarrow y|1) \tag{4}$$

$$\text{PA} \vdash \forall y(y|1 \rightarrow y = 1) \tag{5}$$

$$\text{PA} \vdash \forall xy(y|x \wedge y|Sx \rightarrow y = 1) \tag{6}$$

□

2.3 Euclid's proof with induction

With a slightly different reasoning, one can provide a proof using induction in the following way.

Proof. By Def. of | and Px it is the case, that

$$\text{PA} \vdash \forall y(y|S1 \rightarrow y > 0 \wedge \exists z(z \times y = S1)) \tag{1}$$

$$\text{PA} \vdash \forall y(y|S1 \rightarrow y = 1 \vee y = S1) \tag{2}$$

$$\text{PA} \vdash P(S1) \tag{3}$$

Furthermore, using lemma 1.3 we conclude that

$$\text{PA} \vdash S1 > 0 \tag{4}$$

$$\text{PA} \vdash \exists y(Py \wedge y > 0) \tag{5}$$

By pure logic in PA we conclude that

$$\text{PA} \vdash \exists y(Py \wedge y > x \rightarrow (\exists y(Py \wedge y|S(\prod_{i=1}^{x+1} p_i) \rightarrow (\forall y(Py \rightarrow y \leq Sx) \rightarrow \exists y(Py \wedge y|\prod_{i=1}^{x+1} p_i \wedge y|S(\prod_{i=1}^{x+1} p_i))) \tag{6}$$

Applying the lemmata 1.4 and 1.5 like in the previous proofs, it follows that

$$\text{PA} \vdash \exists y(Py \wedge y > x \rightarrow (\forall y(Py \rightarrow y \leq Sx) \rightarrow \exists y(Py \wedge y|\prod_{i=1}^{x+1} p_i \wedge y|S(\prod_{i=1}^{x+1} p_i)) \tag{7}$$

$$\text{PA} \vdash \exists y(Py \wedge y|\prod_{i=1}^{x+1} p_i \wedge y|S(\prod_{i=1}^{x+1} p_i)) \rightarrow \bot \tag{8}$$

$$\text{PA} \vdash \forall x(\exists y(Py \wedge y > x) \rightarrow \exists y(Py \wedge y > Sx)) \tag{9}$$

Let $\varphi(x) := \exists y(Py \wedge y > x)$ be the induction-formula, then

$$\text{PA} \vdash \forall x \exists y(Py \wedge y > x) \tag{10}$$

□

3 Comparing the euclidian proofs of IP

3.1 Interpretability Strength

It can be easily seen, that all reasoning of the original version of Euclids proof in 2.1 can be done in $I\Delta_0$, except for one: From Chebyshew it is known, that the function $\prod_{i=1}^{x} p_i$ is growing exponentially (see [D'Aquino, 1992]). But if $I\Delta_0$ proves the totality of a function, then this function is polynomial, as proven in [Parikh, 1971]. So $I\Delta_0$ doesn't prove the totality of $\prod_{i=1}^{x} p_i$ and so doesnt allow us to assume the existence of $\prod_{i=1}^{x} p_i$ for arbitrary x. This can be done at first in $I\Delta_0(exp)$. Also $I\Delta_0(exp) \not\vdash I\Delta_0$. The same is true for the version of the proof in 2.2.
On the other hand, the proof by induction in 2.3 has to be carried out in $I\Sigma_1^0$ as there is no obvious way to restrict the quantifier in $\exists y(Py \wedge y > x)$, so we need at least Σ_1^0-induction. Furthermore $I\Sigma_1^0 \not\vdash I\Delta_0(exp)$.

In terms of interpretability strength, the proofs provided in 2.1 and 2.2 are equally simple, but simpler than the proof provided in 2.3. It remains to be shown, that proofs in the manner of 2.1 and 2.2 can not be translated into each other via a recursive function.

3.2 Proof-theoretic Reduction

...

References

[D'Aquino, 1992] D'Aquino, P. (1992). Local behaviour of the chebyshev theorem in models of idelta0. *The Journal of symbolic logic*, 57(1):12–27.

[Heath, 1908] Heath, S. T. L. (1908). *The thirteen books of Euclid's Elements: Translated from the text of Heiberg with introduction and commentary*. University Press Cambridge.

[Parikh, 1971] Parikh, R. (1971). Existence and feasibility in arithmetic. *The Journal of Symbolic Logic*, 36(3):494–508.